Class number one problem for real quadratic fields of certain type

Kostadinka Lapkova

Abstract

We solve the class number one problem for the 2-parameter family of real quadratic fields $\mathbb{Q}(\sqrt{d})$ with square-free discriminant $d = (an)^2 + 4a$ for a and n – positive odd integers, where n is divisible by $43 \cdot 181 \cdot 353$. More precisely, we show that there are no such fields with class number one.

1 Introduction

Let us consider the quadratic fields $K = \mathbb{Q}(\sqrt{d})$ with class group $Cl(d)$ and order of the class group denoted by $h(d)$. In this paper we solve the class number one problem for a subset of the fields $K = \mathbb{Q}(\sqrt{d})$ where $d = (an)^2 + 4a$ is square-free and a and n are positive odd integers with class number $h(d) = 1$. It is known that there are only a finite number of these fields after Siegel's theorem but as the latter is ineffective it is not applicable to finding the specific fields. For this sake we apply the methods developed by Biró in [B1] and in his joint work with Granville [BG].

We remark that the class number one problem that we consider was already suggested by Biró in [B3] as a possible generalization of his works. The discriminant we regard is of Richaud-Degert type with $k = 4$, i.e. $d = (an)^2 + ka$ for $\pm k \in \{1, 2, 4\}$. The class number one problem for special cases of Richaud-Degert type is solved in [B1],[B2],[BY1] and [L] where the parameter $a = 1$. However we already cover a subset of Richaud-Degert type that is of positive density and our problem depends on two parameters. Something more, we believe that in the future we can solve the class number one problem for all the rest discriminants of Richaud-Degert type in a similar way using complex characters and computer check as in [B1], [B2].

2010 *Mathematics Subject Classification*: Primary 11R11; Secondary 11R29 , 11R42.
Key words and phrases: class number problem, real quadratic field.

Under the assumption of a Generalized Riemann hypothesis there is a list of principal quadratic fields of Richaud-Degert type, see [M]. Here, however, our main result is unconditional:

Theorem 1.1. *If* $d = (an)^2 + 4a$ *is square-free for* a *and* n *– odd positive integers such that* $43 \cdot 181 \cdot 353 \mid n$*, then* $h(d) > 1$.

In [BG] Biró and Granville give a finite formula for a partial zeta function at 0 in the case of a general real quadratic field and a general odd Dirichlet character. Basically we follow their method in a much simpler situation where the field has a specific form as in Theorem 1.1, the character is real and its conductor divides the parameter n. As it could be expected, to deduce a formula in this special case is much simpler than in the general case.

The idea of the proof of Theorem 1.1 is roughly speaking the following. We arrive to the identity

$$qh(-q)h(-qd) = n\left(a + \left(\frac{a}{q}\right)\right)\frac{1}{6}\prod_{p|q}(p^2-1)\,, \tag{1.1}$$

where $q \equiv 3 \pmod 4$ is square-free, $(q, a) = 1$ and $q \mid n$. We do this after we compute a partial zeta function at 0 at the principal integral ideals for our specific discriminant, take a real character (mod q) and apply the condition $h(d) = 1$. When we use an analogue of Fact B [B1] to determine the value of $\left(\frac{a}{q}\right)$ and see the factorization of q, we can deduce the exact power of 2 which divides the right-hand side of (1.1). Here comes the place to explain the limitation $43 \cdot 181 \cdot 353 \mid n$. In the analysis of (1.1) we see that we can get a contradiction if we choose q in such a way that the class number $h(-q)$ is divisible by a large power of 2. We choose $q = 43 \cdot 181 \cdot 353$ and use that $h(-43 \cdot 181 \cdot 353) = 2^9 \cdot 3$ has indeed a large power of 2 as a factor, e.g. in [BU] not only the order but also the group structure of $Cl(-43 \cdot 181 \cdot 353)$ is given. Then we show that different powers of two divide the two sides of (1.1) and eventually conclude the proof of Theorem 1.1.

2 Notations and structure of the paper

Let χ be a Dirichlet character of conductor q. Consider the fractional ideal I and the zeta function corresponding to the ideal class of I

$$\zeta_I(s, \chi) := \sum_{\mathfrak{a}} \frac{\chi(N\mathfrak{a})}{(N\mathfrak{a})^s} \tag{2.1}$$

where the summation is over all integral ideals $\mathfrak{a}$ equivalent to I in the ideal class group $Cl(d)$.

Let $f(x,y) \in \mathbb{Z}[x,y]$ be a quadratic form $f(x,y) = Ax^2 + Bxy + Cy^2$ with discriminant $D = B^2 - 4AC$.

Denote by $B_\ell(x)$ the Bernoulli polynomial defined by

$$\frac{Te^{Tx}}{e^T - 1} = \sum_{n\geq 0} B_n(x)\frac{T^n}{n!}$$

and introduce the generalized Gauss sum

$$g(\chi, f, B_\ell) := \sum_{0\leq u,v\leq q-1} \chi\left(f(u,v)\right) B_\ell\left(\frac{v}{q}\right) . \tag{2.2}$$

Always by writing χ_q we mean the real primitive Dirichlet character with conductor q, i.e. $\chi_q(m) = \left(\frac{m}{q}\right)$. This way we are interested in square-free q. The notation $\lceil x \rceil$ signifies the least integer not smaller than x and $(x)_q$ – the least nonnegative residue of $x \pmod q$. Throughout the paper by (a,b) we denote the greatest common divisor of the integers a and b. For $m \in \mathbb{Z}$ and $(m,q) = 1$ we use the notation $\overline{m}$ for the multiplicative inverse of m modulo q. The same overlining for $\alpha \in K$ will denote its agebraic conjugate $\overline{\alpha}$ and the exact use should be clear by the context. As usual $\varphi(x)$ and $\mu(x)$ mean the Euler function and the Möbius function. Let us further denote by $p^\alpha \| l$ the fact that $p^\alpha \mid l$ but $p^{\alpha+1} \nmid l$. We also remind that $B_\ell := B_\ell(0)$.

$\mathcal{O}_K$ represents the ring of integers of the quadratic field K ; $P(K)$ – the set of all nonzero principal ideals of $\mathcal{O}_K$ and $P_F(K)$ – the set of all nonzero principal fractional ideals of K. Let $I_F(K)$ be the set of nonzero fractional ideals of K. The norm of an integral ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is the index $[\mathcal{O}_K : \mathfrak{a}]$. The trace of $\alpha \in K$ will be $Tr(\alpha) = \alpha + \overline{\alpha}$. For $\alpha, \beta \in K$ we write $\alpha \equiv \beta \pmod q$ when $(\alpha - \beta)/q \in \mathcal{O}_K$. When $I_1, I_2 \in I_F(K)$ are represented as ratios of two integral ideals as $\mathfrak{a}_1\mathfrak{b}_1^{-1}$ and $\mathfrak{a}_2\mathfrak{b}_2^{-1}$ we say that the ideals I_1 and I_2 are relatively prime and write $(I_1, I_2) = 1$ in the case when $(\mathfrak{a}_1\mathfrak{b}_1, \mathfrak{a}_2\mathfrak{b}_2) = 1$. The element $\beta \in K$ is called *totally positive*, denoted by $\beta \gg 0$, if $\beta > 0$ and its algebraic conjugate $\bar{\beta} > 0$.

The structure of the paper is the following : in the next section §3 we compute (2.2) for real character χ_q. We need it because in §4 we formulate and prove Claim 4.2 for the value of $\zeta_{P(K)}(0,\chi)$ in terms of sum (2.2). The main result there is Corollary 4.4 for the value of $\zeta_{P(K)}(0,\chi_q)$. Further on in §5 we develop a lemma with the help of which Claim 5.1 - the analogue of Fact B in [B1] is proved and at the end in §6 we prove the main Theorem 1.1. We have an Appendix where for the sake of completeness we give the proof of Corrolary 4.2 from [BG] which we state and use in section §4 as it is in [BG].

3 On a generalized Gauss sum

The main statement in this section is

Claim 3.1. *For $(2A, q) = (D, q) = 1$ and even $\ell \geq 2$ we have*

$$g(\chi_q, f, B_\ell) = \chi_q(A) q B_\ell \prod_{p|q} (1 - p^{-\ell}) .$$

Remark 3.2. When ℓ is odd we have $B_\ell = 0$ for every $\ell \geq 3$. By the property of the Bernoulli polynomials $B_n(1-x) = (-1)^n B_n(x)$ one could easily see that $g(\chi, f, B_\ell)$ is divisible by B_ℓ and thus equals zero, unless when $\ell = 1$ and $\chi = \chi_q$.

Proof. Take the summation on v in (2.2) at the first place –

$$g(\chi_q, f, B_\ell) = \sum_{v=0}^{q-1} B_\ell \left(\frac{v}{q} \right) \sum_{u=0}^{q-1} \chi_q(f(u, v)) .$$

Introduce $r := 2Au + Bv$. Since $(2A, q) = 1$ the values of r cover a full residue system modulo q when u does. Also $r^2 = 4A(f(u, v) + Dv^2/4A)$ so we get $\chi_q(f(u, v)) = \bar{\chi}_q(4A)\chi_q(r^2 - Dv^2)$. As χ_q is of order 2, we have $\chi_q = \bar{\chi}_q$ and $\chi_q(4A) = \chi_q(A)$. Therefore $\chi_q(f(u, v)) = \chi_q(A)\chi_q(r^2 - Dv^2)$. Then

$$\begin{aligned} g(\chi_q, f, B_\ell) &= \chi_q(A) \sum_{v=0}^{q-1} B_\ell \left(\frac{v}{q} \right) \sum_{r=0}^{q-1} \chi_q(r^2 - Dv^2) \\ &= \chi_q(A) \sum_{v=0}^{q-1} B_\ell \left(\frac{v}{q} \right) R , \end{aligned} \tag{3.1}$$

where we abbreviated $R := \sum\limits_{0 \leq r \leq q-1} \chi_q(r^2 - Dv^2)$. We will show that for $g = (v, q)$

$$R = \varphi(g) \mu(\frac{q}{g}) . \tag{3.2}$$

Let $q = \prod_i p_i$. Here there is no square of a prime dividing q because χ_q is a primitive character (mod q) which is of second order and $\left(\frac{\cdot}{p^2} \right) = 1$. After the Chinese Remainder Theorem for any polynomial $F(x, y) \in \mathbb{Z}[x, y]$ we have

$$\sum_{u=0}^{q-1} \chi_q(F(u, v)) = \prod_i \sum_{u_i=0}^{p_i-1} \chi_{p_i}(F(u_i, v)) .$$

Therefore it is enough to consider the sum in (3.2) for every $p \mid q$. In this way let $R_p = \sum_{0\le r\le p-1} \chi_p(r^2 - Dv^2)$. Then $R = \prod_{p|q} R_p$.

If $p \mid q/g$, i.e. $(p, v) = 1$, we have

$$\left(\frac{r^2 - Dv^2}{p}\right) = \left(\frac{Dv^2}{p}\right)\left(\frac{\overline{Dv^2}r^2 - 1}{p}\right) = \left(\frac{D}{p}\right)\left(\frac{\overline{Dv^2}r^2 - 1}{p}\right)$$

because $(D, p) = 1$ and then

$$R_p = \sum_{r=0}^{p-1} \chi_p(r^2 - Dv^2) = \left(\frac{D}{p}\right)\sum_{r=0}^{p-1} \chi_p(\overline{D}r^2 - 1)\,. \tag{3.3}$$

If $\left(\frac{\nu}{p}\right) = -1$, then $\{\nu r^2 - 1 : 0 \le r \le p-1\} \cup \{r^2 - 1 : 0 \le r \le p-1\}$ gives us two copies of the full resdiue system $\pmod p$. Then $\sum_{0\le r\le p-1} \chi_p(\nu r^2 - 1) + \sum_{0\le r\le p-1} \chi_p(r^2 - 1) = 2\sum_{0\le r\le p-1} \chi_p(r) = 0$ and therefore

$$\sum_{r=0}^{p-1} \chi_p(\nu r^2 - 1) = -\sum_{r=0}^{p-1} \chi_p(r^2 - 1) = \left(\frac{\nu}{p}\right)\sum_{r=0}^{p-1} \chi_p(r^2 - 1)\,.$$

Clearly when $\left(\frac{\nu}{p}\right) = 1$ we have $\{\nu r^2 - 1 \pmod p : 0 \le r \le p-1\} \equiv \{r^2 - 1 \pmod p : 0 \le r \le p-1\}$. We conclude that

$$\sum_{r=0}^{p-1} \chi_p(\nu r^2 - 1) = \left(\frac{\nu}{p}\right)\sum_{r=0}^{p-1} \chi_p(r^2 - 1)$$

and for the sum on the right-hand side of (3.3) we can finally assume $\overline{D} = 1$. So

$$\begin{aligned} R_p &= \left(\frac{D}{p}\right)\left(\frac{\overline{D}}{p}\right)\sum_{r=0}^{p-1} \chi_p(r^2 - 1) = \sum_{r=0}^{p-1} \chi_p(r-1)\chi_p(r+1) \\ &= \sum_{\substack{r=0\\ r\neq 1}}^{p-1} \chi_p(\overline{r-1})\chi_p(r+1) = \sum_{\substack{r=0\\ r\neq 1}}^{p-1} \chi_p\left(\frac{r+1}{r-1}\right) \\ &= \sum_{\substack{r=0\\ r\neq 1}}^{p-1} \chi_p\left(1 + \frac{2}{r-1}\right) = \sum_{r=1}^{p-1} \chi_p(1 + 2r) = -1\,. \end{aligned}$$

On the other hand, if $p \mid g$, i.e. $p \mid v$, we have $R_p = \sum_{0\le r\le p-1} \chi_p(r^2) = p - 1 = \varphi(p)$ because χ_p is of second order. Combining the results $R_p = -1$ when $p \mid q/g$ and $R_p = \varphi(p)$ when $p \mid g$ we get

$R = R_q = \mu(q/g)\varphi(g)$ which is exactly (3.2).

When we substitute the value of R in (3.1) we get

$$g(\chi_q, f, B_\ell) = \chi_q(A) \sum_{v=0}^{q-1} \mu(q/g)\varphi(g) B_\ell \left(\frac{v}{q}\right) = \chi_q(A)\Sigma_1 \,, \tag{3.4}$$

where we write Σ_1 for the sum on the right-hand side of (3.4). Further on if $V := v/g$ and $Q := q/g$

$$\Sigma_1 = \sum_{g|q} \mu(q/g)\varphi(g) \sum_{\substack{v=0 \\ g=(v,q)}}^{q-1} B_\ell \left(\frac{v}{q}\right) = \sum_{g|q} \mu(q/g)\varphi(g) \sum_{\substack{V=0 \\ (V,Q)=1}}^{Q-1} B_\ell \left(\frac{V}{Q}\right) .$$

Denote

$$\Sigma_2 := \sum_{\substack{V=0 \\ (V,Q)=1}}^{Q-1} B_\ell(\frac{V}{Q}) .$$

Then

$$\Sigma_2 = \sum_{V=0}^{Q-1} B_\ell \left(\frac{V}{Q}\right) \sum_{d|(V,Q)} \mu(d) = \sum_{d|Q} \mu(d) \sum_{\substack{V=0 \\ d|V}}^{Q-1} B_\ell \left(\frac{V}{Q}\right) = \sum_{d|Q} \mu(d) \sum_{V/d=0}^{Q/d-1} B_\ell \left(\frac{V/d}{Q/d}\right) .$$

We make use of the following property of the Bernoulli polynomials §4.1[W]

$$\sum_{N=0}^{k-1} B_\ell \left(t + \frac{N}{k}\right) = k^{-(\ell-1)} B_\ell(kt) . \tag{3.5}$$

Then

$$\sum_{V/d=0}^{Q/d-1} B_\ell \left(\frac{V/d}{Q/d}\right) = (Q/d)^{-(\ell-1)} B_\ell(0) = Q^{-(\ell-1)} B_\ell d^{\ell-1}$$

and

$$\Sigma_2 = Q^{-(\ell-1)} B_\ell \sum_{d|Q} \mu(d) d^{l-1} = Q^{-(\ell-1)} B_\ell \prod_{p|Q} (1 - p^{\ell-1}) .$$

Now

$$\begin{aligned}
\Sigma_1 &= \sum_{g|q} \mu(q/g)\varphi(g) B_\ell Q^{-(\ell-1)} \prod_{p|Q} (1 - p^{\ell-1}) \\
&= B_\ell q^{-(\ell-1)} \sum_{g|q} \varphi(g) g^{\ell-1} \mu(q/g) \prod_{p|(q/g)} (1 - p^{\ell-1}) \\
&= B_\ell q^{-(\ell-1)} \prod_{p|q} (\varphi(p)p^{\ell-1} - (1 - p^{\ell-1})) = B_\ell q^{-(\ell-1)} \prod_{p|q} (p^\ell - 1) \\
&= B_\ell q \prod_{p|q} (1 - p^{-\ell}) .
\end{aligned}$$

Finally we substitute the value of Σ_1 in (3.4) and this proves the claim. $\square$

4 Computation of a partial zeta function

A main tool used in this section will be the following (Corollary 4.2 from [BG])

Lemma 4.1. *Let (e, f) be a $\mathbb{Z}$-basis of $I \in I_F(K)$ for any real quadratic field K, t be a positive integer, $e^* = e + tf$, and assume that $e, e^* \gg 0$. Furthermore, let $\omega = Ce + Df$ with some rational integers $0 \leq C, D < q$, and write $c = C/q$, $d = D/q$, $\delta = (D - tC)_q/q$. Let*

$$Z_{I,\omega,q}(s) = Z(s) := \sum_{\beta \in H} (\beta\bar{\beta})^{-s}$$

with $H = \{\beta \in I : \beta \equiv \omega \pmod{q}, \beta = Xe + Ye^* \text{ with } (X, Y) \in \mathbb{Q}^2, X > 0, Y \geq 0\}$. Then

$$Z(0) = A(1-c) + \frac{t}{2}(c^2 - c - \frac{1}{6}) + \frac{d-\delta}{2} + Tr\left(\frac{-f}{4e^*}\right) B_2(\delta) + Tr\left(\frac{f}{4e}\right) B_2(d)\,,$$

where $A = \lceil tc - d \rceil$.

For the sake of the paper's completeness we give the lemma's proof in the Appendix.

We use that $d \equiv 1 \pmod 4$, so the ring of integers $\mathcal{O}_K$ of the field K is of the type $\mathcal{O}_K = \mathbb{Z}\left[1, (\sqrt{d}+1)/2\right]$. Introduce $\alpha := (\sqrt{d} - an)/2$ – the positive root of

$$x^2 + (an)x - a = 0\,. \tag{4.1}$$

Then $\alpha + \bar{\alpha} = -an$ and $\alpha\bar{\alpha} = -a$.

We will also come across the quadratic forms

$$f_1(x, y) = x^2 + anxy - ay^2 \tag{4.2}$$

and

$$f_2(x, y) = ax^2 + anxy - y^2\,, \tag{4.3}$$

both of which with discriminant $d = (an)^2 + 4a$.

Recall that $P(K)$ is the set of all nonzero principal ideals in $\mathcal{O}_K$ and define the zeta function

$$\zeta_{P(K)}(s, \chi) = \sum_{\mathfrak{a} \in P(K)} \frac{\chi(N\mathfrak{a})}{(N\mathfrak{a})^s}\,.$$

We have

Claim 4.2. *Let $d = (an)^2 + 4a$ be square-free for a, n – odd positive integers with $a > 1$ and $K = \mathbb{Q}(\sqrt{d})$. If q is such a positive integer that $q \mid n$ and $(q, 2a) = 1$, then for any odd Dirichlet character $\chi \pmod q$ we have*

$$\zeta_{P(K)}(0, \chi) = an.g(\chi, f_1, B_2) + n.g(\chi, f_2, B_2)\,.$$

Proof. We know that for $a > 1$ the fundamental unit of K is $\varepsilon_d = 1 - n\bar{\alpha} > 1$, see [BK]. Thus $\overline{\varepsilon}_d = \varepsilon_+ = 1 - n\alpha$ satisfies $0 < \varepsilon_+ < 1$.

Let us take $I \in I_F(K)$ with $(I, q) = 1$ and consider the zeta function

$$\zeta_I^+(s, \chi) = \zeta_{Cl(I)}^+(s, \chi) := \sum_{\mathfrak{a}} \frac{\chi(N\mathfrak{a})}{(N\mathfrak{a})^s}$$

where the sum is over all integral ideals of K which are equivalent to I in the sense that $\mathfrak{a} = (\beta)I$ for some $\beta \gg 0$. We have $N\varepsilon_d = 1$ and then

$$\zeta_I(s, \chi) = \zeta_I^+(s, \chi) + \zeta_{(\alpha)I}^+(s, \chi)\,.$$

It is also clear that $\zeta_{Cl(I)}^+(s, \chi) = \zeta_{Cl(I^{-1})}^+(s, \chi)$ and for the latter

$$\zeta_{I^{-1}}^+(s, \chi) = \sum_{b \in P_I} \frac{\chi(N(bI^{-1}))}{(N(bI^{-1}))^s} = (NI^{-1})^{-s} \sum_{b \in P_I} \chi\left(\frac{Nb}{NI}\right)(Nb)^{-s}$$

where $P_I = \{b \in P_F(K) : b = (\beta) \text{ for some } \beta \in I\,, \beta \gg 0\}$. We also introduce $V = \{\nu \pmod q : \nu \in I \text{ and } (\nu, q) = 1\}$ and $P_{I,\nu,q} = \{b \in P_F(K) : b = (\beta) \text{ for some } \beta \in I\,, \beta \equiv \nu \pmod q \text{ and } \beta \gg 0\}$. Since $q \mid n$ we get $\varepsilon_d = 1 - n\bar{\alpha} \equiv 1 \pmod q$ and $\varepsilon_+ = 1 - n\alpha \equiv 1 \pmod q$. Thus every $b \in P_I$ given by $b = (\beta) = (\beta\varepsilon_+^j)$ belongs to exactly one residue class $\nu \in V$. Then we have

$$\zeta_I^+(s, \chi) = (NI^{-1})^{-s} \sum_{\nu \in V} \sum_{b \in P_{I,\nu,q}} \chi\left(\frac{Nb}{NI}\right)(Nb)^{-s}\,.$$

If we take into account that $(I, q) = 1$ and therefore $(NI, q) = 1$, also $Nb = \beta\overline{\beta}$, we get

$$\zeta_I^+(s, \chi) = (NI^{-1})^{-s} \sum_{\nu \in V} \chi\left(\frac{\nu\bar{\nu}}{NI}\right) \sum_{b \in P_{I,\nu,q}} (\beta\overline{\beta})^{-s}\,.$$

Now assume that the $\mathbb{Z}$-basis of the fractional ideal I is of the form (e, f) where $e > 0$ is a rational integer and $e^* = e\varepsilon_+ = e + tf \gg 0$. Then for every principal ideal $b \in P_{I,\nu,q}$ there is a unique β such that $b = (\beta) = (\beta\varepsilon_+^j)$ for any $j \in \mathbb{Z}$, and $\varepsilon_+^2 < \beta/\bar{\beta} \leq 1$. As ε_+ is irrational number for every $\beta \in K$ there is a unique pair $(X, Y) \in \mathbb{Q}^2$ such that $\beta = Xe + Ye\varepsilon_+ = e(X + Y\varepsilon_+)$. Then from $\bar{\beta}\varepsilon_+^2 < \beta \leq \bar{\beta}$ we get

$$(X + Y\varepsilon_d)\varepsilon_+^2 < X + Y\varepsilon_+ \leq X + Y\varepsilon_d\,.$$

Now it follows easily that $X > 0$ and $Y \geq 0$. Thus any $b \in P_{I,\nu,q}$ can be presented uniquely like $b = (\beta)$ for $\beta = e(X + Y\varepsilon_+)$ where X, Y are nonnegative rationals with $X > 0$.

Note also that for $0 \leq C, D \leq q-1$ the elements $\nu = Ce + Df \in I$ give a complete system of resdues $\nu \pmod q$. Then we have

$$\zeta_I^+(0,\chi) = \sum_{C,D=0}^{q-1} \chi\left(\frac{(Ce+Df)\overline{(Ce+Df)}}{NI}\right) Z_{I,\nu,q}(0)$$

where $Z_{I,\nu,q}(s)$ is defined in Lemma 4.1.

Observe that $\zeta_{P(K)}(s,\chi) = \zeta_{\mathcal{O}_K}(s,\chi)$ and take $I = \mathcal{O}_K = \mathbb{Z}[1, -\alpha]$. Clearly $(\mathcal{O}_K, q) = 1$. Apply Lemma 4.1 with $e^* = \varepsilon_+ = 1 + n(-\alpha)$ so $t = n$. Also $N\mathcal{O}_K = 1$ and $\nu\bar{\nu} = (C - D\alpha)(C - D\overline{\alpha}) = C^2 - (\alpha + \bar{\alpha})CD + \alpha\bar{\alpha}D = C^2 + anCD - aD^2 = f_1(C,D)$. Since $q \mid t$ we have $\delta = (D - tC)_q/q = D/q = d$ and $\lceil tc - d\rceil = tC/q = tc$. Here $Tr(\alpha/4\varepsilon_+) = Tr(-\alpha/4) = an/4$. Hence

$$\begin{aligned}
Z_{\mathcal{O}_K,\nu,q}(0) &= nc(1-c) + \frac{n}{2}(c^2 - c - \frac{1}{6}) + \frac{an}{2}B_2(d)\\
&= -\frac{n}{2}c^2 + \frac{n}{2}c - \frac{n}{2}\frac{1}{6} + \frac{an}{2}B_2(d)\\
&= -\frac{n}{2}(c^2 - c + \frac{1}{6}) + \frac{an}{2}B_2(d) = -\frac{n}{2}B_2(c) + \frac{an}{2}B_2(d)
\end{aligned}$$

and

$$\begin{aligned}
\zeta_I^+(0,\chi) &= \sum_{C,D=0}^{q-1} \chi(C^2 - aD^2)\left(-\frac{n}{2}B_2(c) + \frac{an}{2}B_2(d)\right)\\
&= -\frac{n}{2}\sum_{C,D=0}^{q-1} \chi(C^2 - aD^2)B_2(c) + \frac{an}{2}\sum_{C,D=0}^{q-1} \chi(C^2 - aD^2)B_2(d)\,.
\end{aligned}$$

Now in the first sum make the change of notation $C \leftrightarrow D$ and take into account that $\chi(-1) = -1$.

Then

$$\begin{aligned}
\zeta_I^+(0,\chi) &= \frac{n}{2}\sum_{C,D=0}^{q-1}\chi(-D^2+aC^2)B_2(d)+\frac{an}{2}\sum_{C,D=0}^{q-1}\chi(C^2-aD^2)B_2(d)\\
&= \frac{n}{2}\sum_{C,D=0}^{q-1}\chi(f_2(C,D))B_2(\frac{D}{q})+\frac{an}{2}\sum_{C,D=0}^{q-1}\chi(f_1(C,D))B_2(\frac{D}{q})\\
&= \frac{an}{2}g(\chi,f_1,B_2)+\frac{n}{2}g(\chi,f_2,B_2)\,. \qquad (4.4)
\end{aligned}$$

Next we find $\zeta^+_{(\alpha)I}(0,\chi)$ after we again apply Lemma 4.1 for $(\alpha)I$. Here again $((\alpha)\mathcal{O}_K,q)=1$. Clearly this follows from $\alpha\overline{\alpha}=a\in(\alpha)\mathcal{O}_K$ and $(a,q)=1$. We can take $\mathcal{O}_K=\mathbb{Z}[-\overline{\alpha},-1]$. Then $(\alpha)\mathcal{O}_K=\mathbb{Z}[-\alpha\overline{\alpha},-\alpha]=\mathbb{Z}[a,-\alpha]$. In this case $\nu\bar{\nu}=(Ca+D(-\alpha))(Ca+D(-\overline{\alpha}))=\alpha\overline{\alpha}(C\bar{\alpha}+D)(C\alpha+D)=-a(-aC^2-anCD+D^2)=af_2(C,D)$. Here $N((\alpha)\mathcal{O}_K)=|\alpha\bar{\alpha}|=a$ and $\chi\left(\nu\bar{\nu}/N((\alpha)I)\right)=\chi(f_2(C,D))=\chi(aC^2-D^2)$. Also $e^*=a\varepsilon_+=a+an(-\alpha)=a(1-n\alpha)$ so $t=an$. Note that again $q\mid t$. Here $Tr(\alpha/4a\varepsilon_+)=Tr(-\alpha/4a)=n/4$ and therefore

$$\begin{aligned}
Z_{(\alpha)\mathcal{O}_K,\nu,q}(0) &= anc(1-c)+\frac{an}{2}(c^2-c-\frac{1}{6})+\frac{n}{2}B_2(d)\\
&= -\frac{an}{2}c^2+\frac{an}{2}c-\frac{an}{2}\frac{1}{6}+\frac{n}{2}B_2(d)\\
&= -\frac{an}{2}(c^2-c+\frac{1}{6})+\frac{n}{2}B_2(d)=-\frac{an}{2}B_2(c)+\frac{n}{2}B_2(d)\,.
\end{aligned}$$

Thus we get

$$\begin{aligned}
\zeta^+_{(\alpha)I}(0,\chi) &= -\frac{an}{2}\sum_{C,D=0}^{q-1}\chi(aC^2-D^2)B_2(c)+\frac{n}{2}\sum_{C,D=0}^{q-1}\chi(aC^2-D^2)B_2(d)\\
&= \frac{n}{2}g(\chi,f_2,B_2)+\frac{an}{2}(-1)\sum_{C,D=0}^{q-1}\chi(aD^2-C^2)B_2(d)\\
&= \frac{n}{2}g(\chi,f_2,B_2)+\frac{an}{2}g(\chi,f_1,B_2)\,. \qquad (4.5)
\end{aligned}$$

Note that we got the equality $\zeta_I^+(0,\chi)=\zeta^+_{(\alpha)I}(0,\chi)$ – an equation that holds true in most general real quadratic fields with $N\epsilon=1$ and χ – an odd character. When we sum up the two zeta functions (4.4) and (4.5) we obtain the statement of the claim. □

Remark 4.3. Here the result on the zeta function at the class of principal integral ideal is for any odd Dirichlet character modulo q. If $a=1$ we have that $N\varepsilon=-1$. In this case $\zeta_I(s,\chi)=\zeta_I^+(s,\chi)$ because for any principal ideal there is a totally positive generator.

From q – odd square-free, $q \mid n$ and $(q,a) = 1$ it follows that $(q,d) = 1$. When we combine Claim 3.1 with Claim 4.2 with the remark $B_2 = 1/6$ we arrive at

Corollary 4.4. *Let $d = (an)^2 + 4a$ be a square-free discriminant for a, n – odd positive integers with $a > 1$ and $K = \mathbb{Q}(\sqrt{d})$. If $q \equiv 3 \pmod 4$ is such a square-free positive integer that $q \mid n$ and $(q, 2a) = 1$, then*

$$\zeta_{P(K)}(0, \chi_q) = \frac{q}{6} n(a + \chi_q(a)) \prod_{p \mid q} (1 - p^{-2})\,.$$

5 Small primes are inert when $h(d) = 1$

In this section we will prove the following result generalizing Fact B in [B1]

Claim 5.1. *If $h(d) = 1$ for the square-free discriminant $d = (an)^2 + 4a$, then a and $an^2 + 4$ are primes. Something more, for any prime $r \neq a$ such that $2 < r < an/2$ we have*

$$\left(\frac{d}{r}\right) = -1\,.$$

We introduced α as the positive root of equation (4.1). Let $\overline{\alpha} = -(an + \sqrt{d})/2$ be the algebraic conjugate of α. We note that $(1, \overline{\alpha})$ form a $\mathbb{Z}$-basis of $\mathcal{O}_k$ with

$$\begin{pmatrix} 1 \\ \overline{\alpha} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{-an+1}{2} & -1 \end{pmatrix} \begin{pmatrix} 1 \\ \frac{\sqrt{d}+1}{2} \end{pmatrix}.$$

For the fundamental unit $\epsilon_d > 1$ the system $(1, \overline{\epsilon}_d)$ was used in [B1] but it forms a basis of the ring $\mathcal{O}_K$ over $\mathbb{Z}$ only when $n = 1$. That is why we need to use different base system. Since

$$\begin{pmatrix} \epsilon_d \\ \overline{\alpha} \end{pmatrix} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \overline{\alpha} \end{pmatrix}$$

with determinant of transformation equal to 1 we can take $(\epsilon_d, \overline{\alpha})$ as a basis of the ring $\mathcal{O}_K$ over $\mathbb{Z}$.

We also have $\epsilon_d \overline{\epsilon}_d = 1$ and

$$\epsilon_d + \overline{\epsilon}_d = 1 - n\alpha + 1 - n\overline{\alpha} = 2 - n(\alpha + \overline{\alpha}) = 2 + an^2\,. \tag{5.1}$$

Here we will reveal some of the splitting behaviour of the primes in the field K.

Lemma 5.2. *If β is an algebraic integer in K such that $|\beta\overline{\beta}| < an/2$, then $|\beta\overline{\beta}|$ is either divisible by a square of a rational integer greater than 1, or equals 1, or equals a.*

Proof. It is enough to prove the claim for

$$1 < |\beta| < \epsilon_d \,. \tag{5.2}$$

Indeed, if $|\beta| = 1$ or $|\beta| = \epsilon_d$ we have $|\beta\overline{\beta}| = 1$ and the statement is true. If $0 < |\beta| < 1$ or $|\beta| > \epsilon_d$ there is an integer k such that $\epsilon_d^{k-1} \leq |\beta| < \epsilon_d^k$, $k < 0$ in the first case and $k > 0$ - in the second. Then $\gamma := \epsilon_d^{1-k}\beta$ is in the interval $[1, \epsilon_d)$ and still $|\gamma\bar{\gamma}| = |\beta\bar{\beta}|$.

So further we assume (5.2). Then we can write $\beta = e\epsilon_d + f\overline{\alpha}$. If $e = 0$ then $\beta = f\overline{\alpha}$, $|\beta\bar{\beta}| = f^2 a$ and the claim is true.

Assume that $e > 0$, the negative case being analogous. If $f = 0$ then $\beta = e\epsilon_d$, $|\beta\bar{\beta}| = e^2$ and this fulfils the lemma. If we assume that the coefficient f is negative, from $\overline{\alpha} < 0$ we get $\beta = e\epsilon_d + f\overline{\alpha} > e\epsilon_d \geq \epsilon_d$ which is out of our range of consideration. Therefore $f > 0$.

Also notice that

$$\beta\bar{\beta} = (e\epsilon_d + f\overline{\alpha})(e\bar{\epsilon}_d + f\alpha) = e^2 + ef(\alpha\epsilon_d + \bar{\alpha}\bar{\epsilon}_d) - af^2.$$

We see that $\alpha\epsilon_d + \bar{\alpha}\bar{\epsilon}_d = \alpha(1 - n\bar{\alpha}) + \bar{\alpha}(1 - n\alpha) = \alpha + \bar{\alpha} - 2n\alpha\bar{\alpha} = -an + 2an = an$. Therefore

$$\beta\bar{\beta} = Q(e, f) := e^2 + (an)ef - af^2 \,. \tag{5.3}$$

where $Q(e, f) = f_2(e, f)$.

We look at the quadratic form $Q(x, y)$. By (5.3) we have that

$$\left| \begin{array}{l} Q_x^{'} = 2x + any \\ Q_y^{'} = anx - 2ay \end{array} \right. \tag{5.4}$$

and this yields that the local extremum of the form is at $x = -any/2$ and $-(an)^2 y/2 = 2ay$. The latter is true only for $y = 0$ but this is out of the considered range where $x, y \geq 1$. That is why for any bounded region of interest in $\mathbb{R}^2$ the extrema would be at its borders. Also $Q_x' > 0$ and therefore for a fixed argument y the function $Q(x, \underline{y})$ is increasing. On the other hand $Q_y'' = -2a < 0$. Thus for fixed x the function $Q(\underline{x}, y)$ has its maximum at $y = nx/2$.

We will investigate the form $Q(x, y)$ according to its sign. We show that it depends on the size of the coefficient f. For example if $f = en$, then $Q(e, f) = e^2 + anfe - af^2 = e^2 + af^2 - af^2 = e^2$ and the lemma is fufilled. Further we consider

Case I : $f < ne$ **.** Here we have $Q(e,f) = e^2 + anfe - af^2 = e^2 + af(ne - f) > e^2 > 0$. On the other hand from $\bar{\alpha} < 0$ it follows that $f\bar{\alpha} > ne\bar{\alpha}$ and

$$\beta = e\epsilon_d + f\bar{\alpha} > e\epsilon_d + ne\bar{\alpha} = e(1 - n\bar{\alpha}) + en\bar{\alpha} = e \geq 1$$

and $\beta = |\beta| < \epsilon_d$ yields

$$1 \leq e < \beta < \epsilon_d < 2 + an^2\,.$$

The latter estimate follows from (5.1) and $0 < \overline{\epsilon_d} < 1$. Thus in the case we regard we are in a region R_1

$$R_1 : \left| \begin{array}{lcl} 1 & \leq e \leq & 1 + an^2 \\ 1 & \leq f \leq & ne - 1 \end{array} \right. \tag{5.5}$$

First assume that $n \geq 3$.

We explained earlier that the maximum of $Q(\underline{x}, y)$ for a fixed argument x is at the line $y = nx/2$. Then $1 < n/2 < n - 1$ and $\min_{R_1} Q(x,y)$ could be at the lines $l_1 : y = 1$ or $l_2 : y = nx - 1$. We are interested in the behaviour of the quadratic form on the latter lines. Since $Q(x, \underline{y})$ is increasing for fixed positive y we have $\min_{l_1} Q(x,y) = Q(1,1)$. On the other hand on l_2 we have

$$\begin{aligned} Q(x, nx-1) &= x^2 + anx(nx-1) - a(nx-1)^2 \\ &= x^2 + a(nx)^2 - anx - a(nx)^2 + 2anx - a = x^2 + anx - a\,. \end{aligned} \tag{5.6}$$

The local extrmemum of this function is achieved when $Q'_x(x, nx-1) = 2x + an = 0$ and $Q''_x(x, nx-1) = 2 > 0$ so it is minimum at $x = -an/2$. This means that for positive x the function $Q(x, nx-1)$ is increasing and thus by (5.6) $\min_{l_2} Q(x,y) = Q(1, n-1) = 1 + an - a = Q(1,1)$. Therefore $\min_{R_1} Q(x,y) = 1 + an - a$. By the condition of the Lemma we know that $an/2 > |\beta\bar{\beta}| = |Q(e,f)| = Q(e,f)$. This is true for the smallest value of the quadratic form in the regarded region as well, i.e. $an/2 > 1 + an - a$. Then we need $a - 1 > an/2$. But for $n \geq 3$ this gives $a - 1 > an/2 > a$ - a contradiction.

From the definition of the discrimnant d we know that n is odd, so $n \neq 2$. Now assume that $n = 1$. We cannot have $e = 1$, otherwise $1 \leq f < en = 1$. Thus $e \geq 2$ and we take up the region R_1 with this correction. Then $1 \leq nx/2 \leq nx - 1$ holds since $1 \leq x/2 \leq x - 1$ for $x \geq 2$. Hence again the minimum is at the very left points of l_1 and l_2, i.e. $\min_{R_1} Q(x,y) = Q(2,1)$. This after (5.6) equals $4 + 2a - a = 4 + a$. Clearly $a > a/2 > 4 + a$ again gives contradiction. We conclude that case I is not possible.

Case II: $f > ne$, in other words $ne - f \le -1$. Suppose that $Q(e,f) > 0$. Then $0 < Q(e,f) = e^2 + anef - af^2 = e^2 + af(ne - f) \le e^2 - af$. Consequently $e^2 > af > ane$ and $e > an$. On the other hand, using that $\alpha > 0$, we get $\bar{\beta} = e\bar{\epsilon}_d + f\alpha > e(1 - n\alpha) + en\alpha = e \ge 1$. So after (5.2)

$$an > an/2 > |\beta\bar{\beta}| = |\beta|.|\bar{\beta}| \ge |\bar{\beta}| = \bar{\beta} > e\,. \tag{5.7}$$

We got $an > e > an$ - a contradiction. Therefore always when $f > ne$ the form $Q(x,y)$ is negative and $e < an/2 \le an - 1$. The last inequality is not fulfilled only when $an = 1$. But in this case $an/2 = 1/2 > |Q(e,f)| = |\beta\bar{\beta}|$ implies that $\beta = 0$ because β is algebraic integer and its norm is integer. Therefore $an > 2$ and we can regard the region

$$R_2 : \left| \begin{array}{rcl} 1 & \le e \le & an - 1 \\ ne + 1 & \le f & \end{array} \right. \tag{5.8}$$

Clearly $|Q(x,y)| = -Q(x,y) = -x^2 - anxy + ay^2 > 0$ and after (5.4) it has extremum out of R_2. Notice that for a fixed x the derivatives $-Q'_y(\underline{x},y) = -anx + 2ay$ and $-Q''_y(\underline{x},y) = 2a > 0$, so at $y = nx/2 < nx + 1$ we have minimum of $-Q(\underline{x},y)$. Therefore $-Q(\underline{x},y)$ is increasing on the lines $x = const$ and we search for the minimum of $-Q(x,y)$ on the line $l_3 : y = xn + 1$.

On the line l_3 we have

$$\begin{aligned} -Q(x, nx+1) &= -x^2 - anx(nx+1) + a(nx+1)^2 = \\ &= -x^2 - a(nx)^2 - anx + a(nx)^2 + 2anx + a = -x^2 + anx + a \end{aligned} \tag{5.9}$$

and at $x = an/2$ we have maximum. So

$$\min_{R_2} |Q(x,y)| = \min\left(-Q(1, n+1), -Q(an-1, n(an-1)+1)\right) .$$

From (5.9) we see that $-Q(1, n+1) = -1 + an + a$ and $-Q(an-1, n(an-1)+1) = -(an-1)^2 + an(an-1) + a = an - 1 + a$, so $\min_{R_2} |Q(x,y)| = -1 + a + an$. Here by the lemma condition $an > -1 + a + an$ and $0 > -1 + a$ or $1 > a$ which is impossible. □

Remark 5.3. If β is an algebraic integer in K such that $|\beta\overline{\beta}| < n\sqrt{a}$ then $|\beta\overline{\beta}|$ is either divisible by a square of a rational integer, or equals 1, or equals a.

This follows easily if we notice that the finer estimate $an/2 > |\beta\bar{\beta}|$ needed for R_1 with $n \ge 3$ could be substituted by

$$n\sqrt{a} > |\beta\bar{\beta}| > 1 + an - a\,.$$

Indeed $n\sqrt{a} > 1 + an - a \Leftrightarrow a - 1 > n\sqrt{a}(\sqrt{a} - 1) \Leftrightarrow (\sqrt{a} - 1)(\sqrt{a} + 1) > n\sqrt{a}(\sqrt{a} - 1)$. If $a = 1$ then $1.n > 1 + 1.n - 1$ is not true. Then $a > 1$ and we get by dividing by $\sqrt{a} - 1 > 0$ the inequality $\sqrt{a} + 1 > n\sqrt{a}$. This yields $2 > 1 + 1/\sqrt{a} > n \ge 3$.

For the other cases we showed that the stronger $an > \min Q(e,f)$ is impossible, so if we assume the statement of the remark with $n\sqrt{a} > Q(e,f)$ it would yield $an > \min Q(e,f)$ - again a contradiction.

Here we give

Proof of Claim 5.1. By Gauss genus theory/e.g. [H]/ it follows that $h(d) = 1$ only if the discriminant d is prime or a product of two primes. Hence the first statement of the claim.

Now let r is prime such that $2 < r < an/2$ and $r \neq a$. Assume $\left(\dfrac{d}{r}\right) = 0$. This means that the prime r ramifies in K and there is a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ for which $r\mathcal{O}_K = \mathfrak{p}^2$. But as the class number is 1, $\mathcal{O}_K$ is a PID and there is $\beta \in \mathcal{O}_K$ such that $\mathfrak{p} = (\beta)$. Then $|\beta\bar{\beta}| = N(\mathfrak{p}) = r < an/2$. By Lemma 3 there is a square of an integer dividing the prime r except for $|\beta\bar{\beta}| = 1$, but then β is a unit and $\mathfrak{p} = \mathcal{O}_K$ - contradiction.

Assume that $\left(\dfrac{d}{r}\right) = 1$. Then there are two prime ideals $\mathfrak{p}_1 \neq \mathfrak{p}_2$ such that $(r) = \mathfrak{p}_1\mathfrak{p}_2$ and $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = r$. But $h(d) = 1$ and $\mathfrak{p}_1 = (\beta)$ for some nonzero $\beta \in \mathcal{O}_K$. Therefore $N(\mathfrak{p}_1) = |\beta\overline{\beta}| = r < an/2$ and by the upper lemma and $r \neq a$, $r > 2$, we have that $|\beta\bar{\beta}|$ is divided by a square of integer $z > 1$. This contradicts the choice of r to be prime.

We got that it is impossible to have $\left(\dfrac{d}{r}\right) = 1$. □

Remark 5.4. When $a = 1$ we have $d = n^2 + 4$ and $h(d) = 1$ yields d to be prime and for any prime $2 < r < n$

$$\left(\frac{n^2+4}{r}\right) = -1\,.$$

Something more, n is also prime.

The first part of the claim can be seen after we apply the same argument as in the proof of Claim 5.1 but with Remark 5.3 instead of Lemma 5.2. Actually in this fashion we got Fact B from [B1]. We see from Corollary 3.16 in [BK] that n is prime if the class number is 1.

6 Proof of Theorem 1.1

Assume that we are in a field $K = \mathbb{Q}(\sqrt{d})$ with $d = (an)^2 + 4a$ with a, n – odd positive integers, $43 \cdot 181 \cdot 353$ divides n and the class number $h(d)$ equals 1. Then all integral ideals are principal and for the Dedekind zeta function

$$\zeta_K(s,\chi) = \sum_{\mathfrak{a}\subset\mathcal{O}_K} \frac{\chi(N\mathfrak{a})}{(N\mathfrak{a})^s}$$

we have $\zeta_K(s,\chi) = \zeta_{P(K)}(s,\chi)$. We know from §4.3 of [W] that

$$\zeta_K(s,\chi) = L(s,\chi)L(s,\chi\chi_d)\,.$$

By the class number formula for imaginary quadratic fields /Theorem 152 in [H]/, again §4.3 of [W], and by $\chi_q(-1) = -1$ because $q \equiv 3 \pmod 4$, we get

$$-L(0,\chi_q) = \sum_{1\le x\le q-1} \frac{x}{q}\left(\frac{x}{q}\right) = h(-q)\,. \tag{6.1}$$

For $d \equiv 1 \pmod 4$ we have $\left(\frac{-1}{d}\right) = (-1)^{(d-1)/2} = 1$ and thus χ_d is an even characater. Hence $\chi_q\chi_d$ is odd character and $L(0,\chi_q\chi_d) = -h(-qd)$. Therefore

$$\zeta_{P(K)}(0,\chi_q) = L(0,\chi_q)L(0,\chi_q\chi_d) = h(-q)h(-qd)\,. \tag{6.2}$$

First think of a general parameter $q \ne a$ that is a prime number, $q \mid n$ and $2 < q < an/2$. Then after Claim 5.1 we have $\left(\frac{d}{q}\right) = -1$. When $q \mid n$ we get $\left(\frac{an^2+4}{q}\right) = \left(\frac{4}{q}\right) = 1$ and $\left(\frac{d}{q}\right) = \left(\frac{a}{q}\right)\left(\frac{an^2+4}{q}\right) = \left(\frac{a}{q}\right) = -1$. That is why the case $a = 1$ is not possible : clearly $\left(\frac{1}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{d}{q}\right) = 1$. So we have $a > 1$.

Now, assume that $43\cdot 181\cdot 353 \mid n$ and $353 < an/2$. Notice that above the prime $a = q$ was not considered because of Claim 5.1. However $\left(\frac{43}{181}\right) = 1$, thus $a = 43$ is not possible; $\left(\frac{181}{43}\right) = 1$ and $\left(\frac{353}{43}\right) = 1$, so $a = 181$ and $a = 353$ are also excluded from our assumptions. Hence, if $353 < an/2$ and $43, 181, 353 \mid n$, the class number $h(d) = 1$ only if $\left(\frac{a}{43}\right) = \left(\frac{a}{181}\right) = \left(\frac{a}{353}\right) = -1$.

Now we take the parameter $q = 43\cdot 181\cdot 353$. Again consider the real primitive character $\chi_q(m) = \left(\frac{m}{q}\right)$ modulo q. As $43 \equiv 3 \pmod 4$, $181 \equiv 1 \pmod 4$ and $353 \equiv 1 \pmod 4$ we have $q \equiv 3 \pmod 4$ and $\chi_q(-1) = -1$. Also $a > 1$ and we can apply (6.2) and Corollary 4.4 and multiply both sides of its equation by q. This way we arrive at the promised equation (1.1)

$$qh(-q)h(-qd) = n\left(a + \left(\frac{a}{q}\right)\right)\frac{1}{6}\prod_{p\mid q}(p^2-1)\,.$$

In this case

$$B := \frac{1}{6}\prod_{p|q}(p^2-1) = \frac{1}{6}42\cdot 44\cdot 180\cdot 182\cdot 352\cdot 354 = 2^{11}3^3\dots$$

and $2^{11}\|B$.

As $a>1$ we have that $d=a(an^2+4)$ is product of two different primes. Notice as well that $a\equiv an^2+4 \pmod 4$. By the genus theory /e.g. Theorem 134 in [H]/ we know that if $a\equiv an^2+4\equiv 1 \pmod 4$ for the real quadratic field $K=\mathbb{Q}(\sqrt{a(an^2+4)})$, then the 2-rank of the class group is the same as of the 2-rank of the narrow class group, i.e. $2-1=1$. This contradicts $h(d)=1$. Therefore $a\equiv 3 \pmod 4$. But in this case $a+\left(\frac{a}{q}\right)=a-1$ and $a-1\equiv 2 \pmod 4$ so $2\|\left(a+\left(\frac{a}{q}\right)\right)$. Here Claim 5.1 plays a great importance, also q being factor of three primes, for then $\left(\frac{a}{q}\right)=-1$. The parameter n is odd by definition. It follows that for the right-hand side of (1.1) we have

$$2^{12}\|n\left(a+\left(\frac{a}{q}\right)\right)B\,. \tag{6.3}$$

We regard the left-hand side of (1.1). As we pointed out in §1 we have $h(-43\cdot 181\cdot 353)=2^9\cdot 3$. Again by genus theory/Theorem 132, [H]/ the 2-class group of $Cl(-qd)$ has a rank $5-1=4$ since qd has 5 distinct prime divisors. Indeed, we showed that $a\notin\{43,181,353\}$, also $an^2+4>an/2>353$ and clearly $a\neq an^2+4$. Therefore $2^{9+4}=2^{13}\mid qh(-q)h(-qd)$. This contradicts (6.3).

We conclude that $h(d)>1$ for $an/2>353$. But then for discriminants $d=(an)^2+4a$ for positive odd a and n and $43\cdot 181\cdot 353\mid n$ we cannot have class number 1. This concludes the proof of Theorem 1.1.

Remark 6.1. The main idea used in this paper - comparison of 2-parts in (1.1), can be utilized toward other results of this type. For example, if $d=a(an^2+4)$ for a and n – odd positive integers where $5\cdot 359\cdot 541\mid n$, then $h(d)>1$. The exact divisors of n are chosen according to Table 12 in [BU]: $h(-5\cdot 359\cdot 541)=2^9$ and again we have a bigger power of 2 on the left-hand side of (1.1). Also $5\cdot 359\cdot 541\equiv 3 \pmod 4$ so when we take up a real character we have formula (6.1). Also $a\in\{5,359,541\}$ are not covered by Claim 5.1 for each prime in the set, but these a's are excluded by a simple check of the Legendre symbols of each other.

In this sense in an upcoming paper we generalize the result in [BY2] for discriminant with three prime divisors, thus extending our Theorem 1.1 for an infinite family of n such that $pqr \mid n$.

7 Appendix

The proof here represents word for word the proof of Corollary 4.2 in [BG]. We give it in order to keep the present paper as self-contained as possible.

Proof of Lemma 4.1. As it was first realized in [B1], the value of the function $Z_{I,\omega,q}(0)$ in the Yokoi's case $a = 1$ can be computed using a result of Shintani. This is also the way in the most general case of real quadratic field K that Lemma 4.1 treats.

Let for the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with positive elements and $x > 0, y \geq 0$ we define the zeta function

$$\zeta\left(s, \begin{pmatrix} a & b \\ c & d \end{pmatrix}, (x,y)\right) := \sum_{n_1,n_2=0}^{\infty} (a(n_1+x)+b(n_2+y))^{-s}(c(n_1+x)+d(n_2+y))^{-s}\,.$$

Then we have

Claim 7.1 (Shintani). *For any $a, b, c, d, x > 0$ and $y \geq 0$ the function $\zeta\left(s, \begin{pmatrix} a & b \\ c & d \end{pmatrix}, (x,y)\right)$ is absolutely convergent for $\Re s > 1$, extends meromorphically to the whole complex plane and*

$$\zeta\left(s, \begin{pmatrix} a & b \\ c & d \end{pmatrix}, (x,y)\right) = B_1(x)B_1(y) + \frac{1}{4}\left(B_2(x)\left(\frac{c}{d}+\frac{a}{b}\right) + B_2(y)\left(\frac{d}{c}+\frac{b}{a}\right)\right)\,.$$

Note that $A = \left\lceil \frac{tC-D}{q} \right\rceil = \frac{tC-D+q\delta}{q} = tc - d + \delta$ and therefore $0 \leq A \leq t$. Let $\beta = Xe + Ye^*$ for some rationals $X > 0, Y \geq 0$. Write $X = qx + qn_1$ and $Y = qy + qn_2$ for some nonnegative integers n_1 and n_2 and rational numbers $0 < x \leq 1\,, 0 \leq y < 1$ which can be done in a unique way. Then on the one hand,

$$\beta\bar{\beta} = q^2\left(e(n_1+x) + e^*(n_2+y)\right)\left(\bar{e}(n_1+x) + \overline{e^*}(n_2+y)\right)$$

and on the other hand we have that $\beta \in I$ and $\beta \equiv \omega \pmod{q}$ hold if and only if $xe+ye^*-(ce+df) \in I$. Therefore

$$Z(s) = \frac{1}{q^{2s}} \sum_{(x,y)\in R(C,D)} \zeta\left(s, \begin{pmatrix} e & e^* \\ \bar{e} & e^* \end{pmatrix}, (x,y)\right)$$

where $R(C,D) := \{(x,y) \in \mathbb{Q}^2 : 0 < x \leq 1\,, 0 \leq y < 1\,, xe + ye^* - (ce+df) \in I\}$. Therefore by Claim 7.1 we get

$$Z(0) = \sum_{(x,y)\in R(C,D)} \left(B_1(x)B_1(y) + Tr\left(\frac{e}{4e^*}\right)B_2(x) + Tr\left(\frac{e^*}{4e}\right)B_2(y)\right)\,.$$

We observe that for any m, n we have

$$\frac{mf+ne}{q} = \frac{(n-\frac{m}{t})e+\frac{m}{t}e^*}{q}$$

and so it is easy to see that the possibilities for (m,n) having $(x,y) \in R(C,D)$ with

$$(x,y) = \left(\frac{1}{q}\left(n-\frac{m}{t}\right), \frac{1}{q}\frac{m}{t}\right)$$

are

$$m_j = D + jq\,, n_j = C + q\left[1+\frac{j}{t}-\frac{(tC-D)/q}{t}\right]$$

with an integer $0 \le j \le t-1$. This is so because the possible values of m are obviously these t values, and once m is fixed, n is unique. Now

$$0 < 1+\frac{j}{t}-\frac{(tC-D)/q}{t} < 2, \text{ so } n_j = \begin{cases} C & \text{if } 0 \le j < A \\ C+q & \text{if } A \le j < t \end{cases},$$

and therefore

$$Z(0) = \sum_{j=0}^{t-1}\left(B_1(x_j)B_1(y_j) + Tr\left(\frac{e}{4e^*}\right)B_2(x_j) + Tr\left(\frac{e^*}{4e}\right)B_2(y_j)\right)$$

where $y_j = \frac{d+j}{t}$ for $0 \le j < t$ and $x_j = \begin{cases} c-y_j & \text{if } 0 \le j < A \\ c+1-y_j & \text{if } A \le j < t \end{cases}$

Now, by (3.5) we have

$$\sum_{j=0}^{t-1} B_2(y_j) = \sum_{j=0}^{t-1} B_2(\frac{d+j}{t}) = \frac{1}{t}B_2(d)$$

and

$$\begin{aligned}\sum_{j=0}^{t-1} B_2(x_j) &= \sum_{j=0}^{A-1} B_2\left(\frac{A-j-\delta}{t}\right) + \sum_{j=A}^{t-1} B_2\left(\frac{t+A-j-\delta}{t}\right) \\ &= \sum_{k=1}^{t} B_2\left(\frac{k-\delta}{t}\right) = \sum_{l=0}^{t-1} B_2\left(\frac{\delta+l}{t}\right) = \frac{1}{t}B_2(\delta)\,.\end{aligned}$$

Now since $B_2(x)+B_2(y)+2B_1(x)B_1(y) = (x+y-1)^2 - 1/6$ we easily deduce that

$$\sum_{j=0}^{t-1}(B_2(x_j)+B_2(y_j)+2B_1(x_j)B_1(y_j)) = A(c-1)^2 + (t-A)c^2 - \frac{t}{6}\,.$$

The result then follows from the last four displayed equations, and the facts that

$$Tr\left(\frac{e}{4te^*}\right) - \frac{1}{2t} = Tr\left(\frac{-f}{4e^*}\right) \text{ and } Tr\left(\frac{e^*}{4te}\right) - \frac{1}{2t} = Tr\left(\frac{f}{4e}\right)\,.$$

□

Acknowledgements.

I would like to thank my supervisor András Biró for introducing me to the class number one problem, for his valuable ideas, proofreading and patient support during the writing of this paper.

References

[B1] A. Biró, *Yokoi's conjecture*, Acta Arith. 106 (2003), no. 1, 85–104

[B2] A. Biró, *Chowla's conjecture*, Acta Arith. 107 (2003), no. 2, 179–194

[B3] A. Biró, *Yokoi-Chowla conjecture and related problems*, Proceedings of the 2003 Nagoya Conference,Held at Nagoya University, Nagoya, October 14–17, 2003, Ed. S. Katayama, C. Levesque and T. Nakahara., Saga University, Faculty of Science and Engineering, Saga, 2004

[BG] A. Biró, A. Granville, *Zeta function for ideal classes in real quadratic fields, at s=0*, preprint

[BU] D. A. Buell, *Class groups of quadratic fields*, Math. Comp. 135 (1976), 610–623

[BK] D. Byeon, H. Kim, *Class number* 1 *criteria for real quadratic fields of Richaud-Degert type.*, J. Number Theory 57 (1996), no. 2, 328–339

[BY1] D. Byeon, M. Kim, J. Lee, *Mollin's conjecture*, Acta Arith. 126 (2007), 99–114

[BY2] D. Byeon, Sh. Lee, *Divisibility of class numbers of imaginary quadratic fields whose discriminant has only two prime factors*, Proc. Japan Acad. 84, Ser. A (2008), 8–10

[H] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer, 1981

[L] J. Lee, *The complete determination of wide Richaud-Degert types which are not 5 modulo 8 with class number one*, Acta Arith. 140 (2009), no. 1, 1–29

[M] R. A. Mollin, H. C. Williams, *Solution of the class number one problem for real quadratic fields of extended Richaud-Degert type (with one possible exception)*, Number theory (Banff, AB, 1988), 417–425, de Gruyter, Berlin, 1990.

[W] L.C. Washington, *Introduction to Cyclotomic Fields*, Springer, 1996